UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

SABLE NETWORKS, INC. AND SABLE IP, LLC, ***Plaintiffs,*** v. **FORCEPOINT LLC,** ***Defendant.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Sable Networks, Inc. and Sable IP, LLC (collectively, "Sable" or "Plaintiffs") bring this action and make the following allegations of patent infringement relating to U.S. Patent Nos.: 6,954,431 (the "'431 patent"); 6,977,932 (the "'932 patent"); 8,243,593 (the "'593 patent"); and 9,774,501 (the "'501 patent") (collectively, the "patents-in-suit"). Defendant Forcepoint LLC ("Forcepoint" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.[1] The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the increasing amount of data sent over computer networks.

[1] Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) ("Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.").

2. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.[2] Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.

Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router,* IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001)("Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency's Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.").

3. Dr. Roberts' work on ARPANET played a key role in the development of packet switching networks. Packet switching is a digital network transmission process in which data is broken into parts which are sent independently and reassembled at a destination. Electronic messages sent over the ARPANET were broken up into packets then routed over a network to a destination. "In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using

[2] Katie Hafner, *Lawrence Roberts, Who Helped Design Internet's Precursor,* N.Y. TIMES at A2 (December 31, 2018) ("Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.").

those tiny data packets to send information from place to place."[3] Packet switching has become the primary technology for data communications over computer networks.

From Two Small Nodes, a Mighty Web Has Grown

By 1966, with these and other basic ideas in place, Lawrence Roberts, recruited by ARPA from the Massachusetts Institute of Technology, mapped out the plan. Two years after the first transmission, the number of host computers grew to 23. The @ symbol was invented in 1972, and a year later 75 percent of the Arpanet traffic was E-mail. It was starting to look like the Net.").

George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

4. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data traversing the internet.[4] Dr. Roberts identified that as the "Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in."[5]

> ***The Internet is broken. I should know: I designed it***. In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data traffic-I called them Interface Message Processors, or IMPs-evolved into today's

[3] Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) ("The ARPANET was, in part, an experimental verification of the packet switching concept. Robert's objective was a new capability for resource sharing.").

[4] eWeek Editors, *Feeling A Little Congested,* EWEEK MAGAZINE (September 24, 2001) ("Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.").

[5] Michael Cooney, *Can ATM Save The Internet,* NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, A RADICAL NEW ROUTER, IEEE Spectrum Vol. 46 34-39 (August 2009).

> routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

5. In 1998, Dr. Roberts founded Caspian Networks.[6] At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This new router was aimed at addressing concerns about network "gridlock." In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. "Roberts says the Apeiro will also create new revenue streams for the carriers by solving the 'voice and video problem.' IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient."[7]

Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight: Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

[6] Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to Caspian Networks, Inc. in 1999.

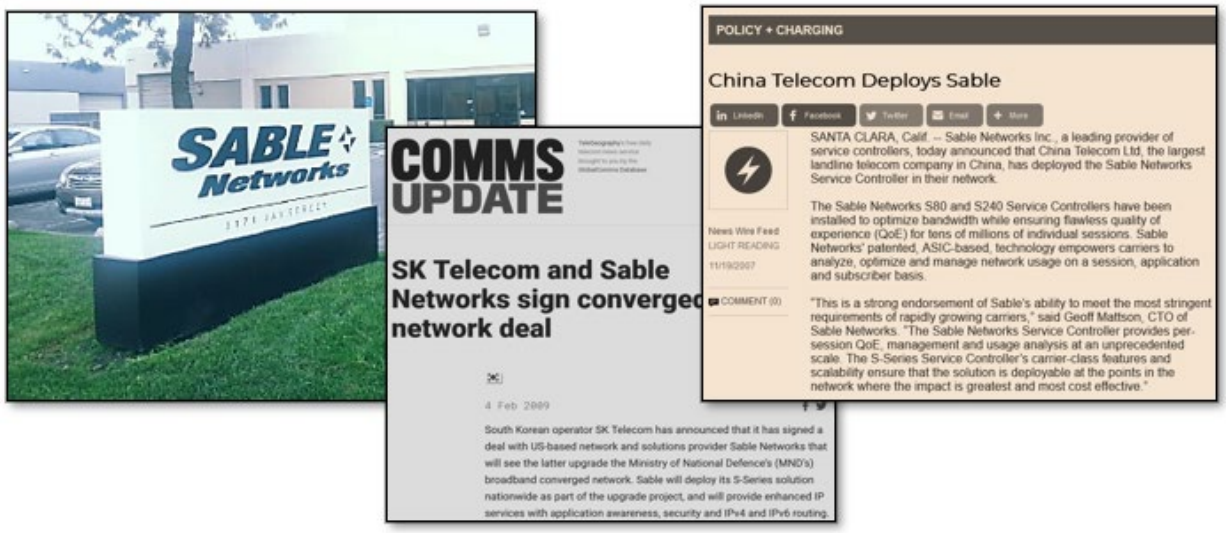
[7] John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE (May 1, 2001).

6. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included numerous technological advances including quality of service (QoS) routing and flow-based routing.

7. At its height, Caspian Networks Inc. raised more than $300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

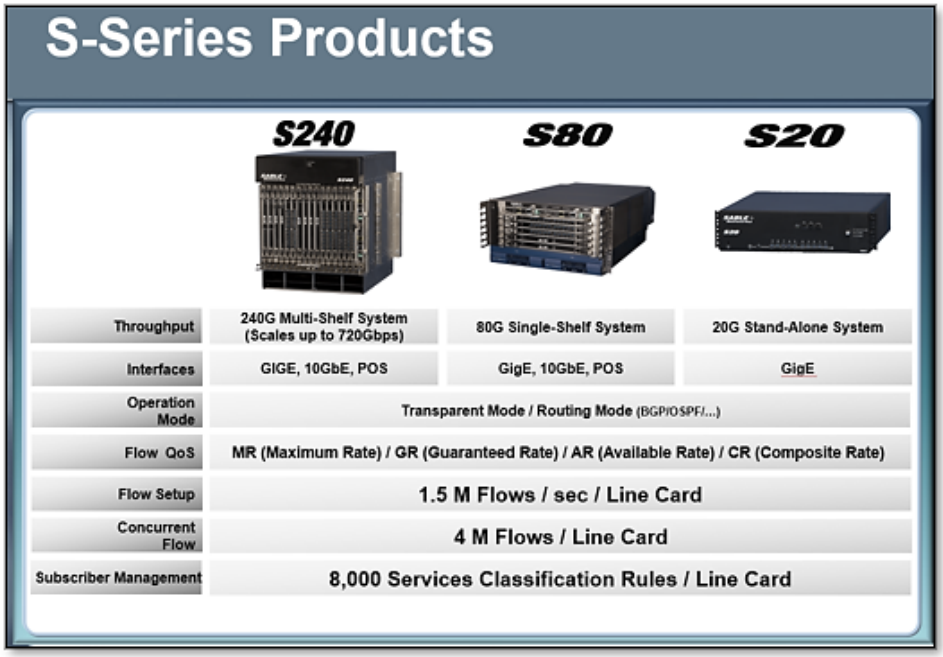
8. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.[8] Sable Networks, Inc. has continued its product development efforts and has gained commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.

[8] Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.



SK Telecom and Sable Networks Sign Convergence Network Deal, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) ("South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks."); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) ("Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.").

9. Armed with the assets of Caspian Networks Inc. as well as members of Caspian Networks' technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts' flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits ("ASIC") designed for flow traffic management. Sable Network, Inc.'s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (*e.g.*, S80 and S240 Service Controller models) that contain Sable Networks' flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.



SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

10. Sable pursues the reasonable royalties owed for Forcepoint's use of the inventions claimed in Sable's patent portfolio, which arise from Caspian Networks and Sable Networks' groundbreaking technology.

SABLE'S PATENT PORTFOLIO

11. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

12. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- Cisco Systems, Inc.[9]
- Juniper Networks, Inc.[10]
- Broadcom Limited[11]
- EMC Corporation[12]
- F5 Networks, Inc.[13]
- Verizon Communications Inc.[14]
- Microsoft Corporation[15]
- Intel Corporation[16]
- Extreme Networks, Inc.[17]
- Huawei Technologies Co., Ltd.[18]

THE PARTIES

SABLE NETWORKS, INC.

13. Sable Networks, Inc. ("Sable Networks") is a corporation organized and existing under the laws of the State of California.

14. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts

[9] *See, e.g.*, U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

[10] *See, e.g.*, U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

[11] *See, e.g.*, U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

[12] *See, e.g.*, U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

[13] *See, e.g.*, U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

[14] *See, e.g.*, U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

[15] *See, e.g.*, U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

[16] *See, e.g.*, U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

[17] *See, e.g.*, U.S. Patent Nos. 7,903,654; 7,978,614; 8,149839; 10,212,224; 9,112,780; and 8,395,996.

[18] *See, e.g.*, U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent Nos. CN108028828 and CN106161333.

to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

15. Sable Networks is the owner by assignment of all of the patents-in-suit.

SABLE IP, LLC

16. Sable IP, LLC ("Sable IP") is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

FORCEPOINT LLC

17. Forcepoint LLC ("Forcepoint"), is a Delaware corporation with its principal place of business at 10900-A Stonelake Blvd., Quarry Oaks 1, Ste. 350, Austin, Texas 78759. Forcepoint may be served through its registered agent Corporate Creations Network Inc., 5444 Westheimer #1000, Houston, Texas 77056. Forcepoint is registered to do business in the State of Texas and has been since at least January 13, 2016.

18. Forcepoint conducts business operations within the Western District of Texas where it sells, develops, and/or markets its products including its headquarters at 10900-A Stonelake Blvd., Quarry Oaks 1, Ste. 350, Austin, Texas 78759.

JURISDICTION AND VENUE

19. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

20. This Court has personal jurisdiction over Forcepoint in this action because Forcepoint has committed acts within the Western District of Texas giving rise to this action and

has established minimum contacts with this forum such that the exercise of jurisdiction over Forcepoint would not offend traditional notions of fair play and substantial justice. Forcepoint is registered to do business in the State of Texas, and maintains its corporate headquarters in Austin, Texas.

21. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Forcepoint is registered to do business in the State of Texas, maintains its corporate headquarters in the Western District of Texas, has transacted business in the Western District of Texas and has committed acts of direct and indirect infringement in the Western District of Texas.

22. Forcepoint has a regular and established place of business in this District and has committed acts of infringement in this District. Forcepoint maintains its corporate headquarters at 10900-A Stonelake Blvd., Quarry Oaks 1, Ste. 350, Austin, Texas 78759, which is located within this District. Forcepoint employs full-time personnel such as sales personnel and engineers in this District. Forcepoint has also committed acts of infringement in this District by commercializing, marketing, selling, distributing, testing, and servicing the Accused Products.

23. This Court has personal jurisdiction over Forcepoint. Forcepoint has conducted and does conduct business within the State of Texas. Forcepoint, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises (including by providing an interactive web page) its products and/or services in the United States and the Western District of Texas and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Western District of Texas. Forcepoint, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has

purposefully and voluntarily placed one or more of its infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Western District of Texas. These infringing products and/or services have been and continue to be made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Western District of Texas. Forcepoint has committed acts of patent infringement within the Western District of Texas. Forcepoint interacts with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, Forcepoint directly infringes the patents-in-suit.

24. Forcepoint has minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over Forcepoint.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,954,431

25. U.S. Patent No. 6,954,431 (the "'431 patent") entitled, *Micro-Flow Management*, was filed on December 6, 2001, and claims priority to April 19, 2000. The '431 patent is subject to a 35 U.S.C. § 154(b) term extension of 722 days. Sable Networks, Inc. is the owner by assignment of the '431 patent. Sable IP is the exclusive licensee of the '431 patent. A true and correct copy of the '431 patent is attached hereto as Exhibit A.

26. The '431 patent discloses novel methods and systems for managing data traffic comprising a plurality of micro-flows through a network.

27. The inventions disclosed in the '431 patent improve the quality of service in data transmissions over a computer network by relying on per micro-flow state information that enables rate and delay variation requirements to be within set quantified levels of service.

28. The ‘431 patent discloses technologies that speed the rate at which data can effectively travel over a computer network by optimizing packet discarding.

29. The ‘431 patent discloses the use of micro-flow state information to determine the rate of each flow, thus optimizing discards and optimizing the quality of service of data transmission.

30. The ‘431 patent discloses methods and systems that avoid networking system degradation by not overloading network switch buffers.

31. The ‘431 patent discloses a method for managing data traffic through a network that determines a capacity of a buffer containing a micro-flow based on a characteristic.

32. The ‘431 patent discloses a method for managing data traffic through a network that assigns an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

33. The ‘431 patent discloses a method for managing data traffic through a network that delegates a portion of available bandwidth in the network to the micro-flow.

34. The ‘431 patent discloses a method for managing data traffic through a network that uses the buffer for damping jitter associated with the micro-flow.

35. The ‘431 patent has been cited by 103 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘431 patent as relevant prior art:

- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Broadcom Limited
- Intel Corporation
- Sun Microsystems, Inc.
- Oracle Corporation
- Samsung Electronics Co., Ltd.
- Adtran, Inc.

- Time Warner Cable, Inc.
- FSA Technologies, Inc.
- Internap Corporation
- France Telecom
- The Boeing Company
- Wistaria Trading, Ltd.

U.S. PATENT NO. 6,977,932

36. U.S. Patent No. 6,977,932 (the "'932 patent") entitled, *System and Method for Network Tunneling Utilizing Micro-Flow State Information*, was filed on January 16, 2002. The '932 patent is subject to a 35 U.S.C. § 154(b) term extension of 815 days. Sable Networks, Inc. is the owner by assignment of the '932 patent. Sable IP is the exclusive licensee of the '932 patent. A true and correct copy of the '932 patent is attached hereto as Exhibit B.

37. The '932 patent discloses novel methods and apparatuses for utilizing a router capable of network tunneling utilizing flow state information.

38. The inventions disclosed in the '932 patent enable the use of micro-flow state information to improve network tunneling techniques.

39. The inventions disclosed in the '932 patent maintain flow state information for various quality of service characteristics by utilizing aggregate flow blocks.

40. The aggregate flow blocks disclosed in the '932 patent maintain micro-flow block information.

41. The technologies claimed in the '932 patent speed the flow of network traffic over computer networks by avoiding time consuming and processor intensive tasks by combining flow state information with other information such as label switched paths utilization information. This permits the micro-flows associated with an aggregate flow block to all be processed in a similar manner.

42. The technologies disclosed in the '932 patent result in more efficient computer networks by avoiding the processor intensive tasks of searching millions of flow blocks to identify flow blocks having certain micro-flow characteristics in order to process large numbers of micro-flows.

43. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing an aggregate flow block having tunnel specific information for a particular network tunnel.

44. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing a flow block having flow state information for a micro-flow, the flow block further including an identifier that associates the flow block with the aggregate flow block.

45. The '932 patent discloses a router capable of network tunneling utilizing flow state information wherein the aggregate flow block stores statistics for the particular network tunnel.

46. The '932 patent has been cited by 86 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '932 patent as relevant prior art:

- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Avaya, Inc.
- Fujitsu, Ltd.
- Intel Corporation
- Nokia Corporation
- Qualcomm, Inc.
- Sprint Communications Co.
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

U.S. PATENT NO. 8,243,593

47. U.S. Patent No. 8,243,593 entitled, *Mechanism for Identifying and Penalizing Misbehaving Flows in a Network*, was filed on December 22, 2004. The '593 patent is subject to

a 35 U.S.C. § 154(b) term extension of 1,098 days. Sable Networks, Inc. is the owner by assignment of the '593 patent. Sable IP is the exclusive licensee of the '593 patent. A true and correct copy of the '593 patent is attached hereto as Exhibit C.

48. The '593 patent discloses novel methods and systems for processing a flow of a series of information packets.

49. The inventions disclosed in the '593 patent teach technologies that permit the identification and control of less desirable network traffic.

50. Because the characteristics of data packets in undesirable network traffic can be disguised, the '593 patent improves the operation of computer networks by disclosing technologies that monitor the characteristics of flows of data packets rather than ancillary factors such as port numbers or signatures.

51. The '593 patent discloses tracking the behavioral statistics of a flow of data packets that can be used to determine whether the flow is undesirable.

52. The '593 patent further discloses taking actions to penalize the flow of undesirable network traffic.

53. The '593 patent discloses a method for processing a flow of a series of information packets that maintains a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

54. The '593 patent discloses a method for processing a flow of a series of information packets that determines, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

55. The ‘593 patent discloses that the determination as to whether the flow is exhibiting undesirable behavior is made regardless of the presence or absence of congestion.

56. The ‘593 patent discloses a method for processing a flow of data packets that enforces a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

57. The ‘593 patent has been cited by 17 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘593 patent as relevant prior art.

- Cisco Systems, Inc.
- AT&T, Inc.
- International Business Machines Corporation
- Telecom Italia S.p.A.
- McAfee, LLC

U.S. PATENT NO. 9,774,501

58. U.S. Patent No. 9,774,501 (the “‘501 patent”) entitled, *System and Method for Ensuring Subscriber Fairness Using Outlier Detection*, was filed on September 7, 2016, and claims priority to May 14, 2012. Sable Networks, Inc. is the owner by assignment of the ‘501 patent. Sable IP is the exclusive licensee of the ‘501 patent. A true and correct copy of the ‘501 patent is attached hereto as Exhibit D.

59. The ‘501 patent claims specific methods and devices for a subscriber fairness solution that uses flow-based statistical collection mechanism to monitor subscriber usage across various attributes.

60. The ‘501 patent discloses methods and systems for detecting outlier users of a network resource.

61. The ‘501 patent teaches technologies for detecting outlier users of a network resource using a fairness model that accounts for the cost of a user's behavior on other users and provides for evaluating and effecting service fairness.

62. The ‘501 patent discloses aggregating flow data of a user of a network resource for set time periods. The flow data that is aggregated can include connections between a particular source IP address and transport layer port to a particular destination IP address and transport layer port.

63. The ‘501 patent discloses applying outlier detection logic to the flow-count pattern that is generated for a user and comparing it to flow-count patterns associated with other users on the network.

64. The ‘501 patent discloses a method of assigning a flow-count band to the user based on the outlier detection logic where the user’s flow count is compared to the flow-count data of other users on the network.

65. The ‘501 patent discloses a method of applying a mitigating action to the user based on the user’s access to the network resource based on the flow-count band that the user’s activity causes the user to be assigned to.

66. The ‘501 patent discloses a method of implementing outlier detection for a user on a network using a detection phase and a mitigation phase. In the detection phase, “outliers” are identified - users that are using a disproportionate amount of network resources. In the mitigation phase, actions are taken to restrict the access of the outlier user to network resources.

67. The ‘501 patent discloses a computer implemented method that improves the function of a computer network through using outlier detection to mitigate an individual user’s over use of the network bandwidth.

68. The '501 patent family has been cited by 11 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '501 patent family as relevant prior art:

- Cisco Systems, Inc.
- International Business Machines Corporation
- Google, Inc.
- Adobe, Inc.
- British Telecomm
- VMware, Inc.
- Sprint Spectrum L.P.
- Infinera Corporation

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,954,431

69. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

70. Forcepoint designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing data traffic comprising a plurality of micro-flows through a network.

71. Forcepoint designs, makes, sells, offers to sell, imports, and/or uses Forcepoint Next Generation Firewall (NGFW) Appliances running Forcepoint NGFW 6.0 and later software, including but not limited to the following: Forcepoint NGFW Appliances (including the following models: NGFW 5206 Appliance, NGFW 1401 Appliance, NGFW 3207 Appliance, NGFW 320X Appliance, NGFW 1402 Appliance, NGFW 1035 Appliance, NGFW 1065 Appliance, NGFW 321 Appliance, NGFW 325 Appliance, NGFW 110 Appliance, NGFW 115 Appliance, NGFW 331 Appliance, NGFW 335W Appliance, NGFW 51 Appliance, NGFW 51 LTE Appliance, NGFW 3301 Appliance, NGFW 3305 Appliance, NGFW 6205 Appliance, NGFW 2101 Appliance, NGFW 2105 Appliance, NGFW SMC 1000 Appliance, NGFW 1101 Appliance, NGFW 1105

Appliance, NGFW 330 Appliance, NGFW 335 Appliance, NGFW 3401 Appliance, NGFW 3405 Appliance, NGFW 3410 Appliance, NGFW 120W Appliance, and NGFW 60 Appliance); Forcepoint S Series Appliance (including the following models: Storage Array 30TB, Storage Array 110TB, and Storage Array 60TB); Forcepoint V10000 Series Appliance (including the following models: V10000 G4 R2, V10000 G4, V20000 G1, V5000 G3, V5000 G4, and V5000 G4 R2); Forcepoint X Series Appliance (including the following models: X10G Blade G2 R2 and X10G Blade G2); and Forcepoint Z Series Appliance (including the following models: Z2500 G1.2, Z5000 G1.2, Z10000 G1.2, Z20000 G1.2, Z50000 G1.2, Z2500 G1.1, Z5000 G1.1, Z10000 G1.1, Z20000 G1.1, Z50000 G1.1, Z2500 G1.0, Z5000 G1.0, Z10000 G1.0, Z20000 G1.0, and Z50000 G1.0) (collectively, the "Forcepoint '431 Products(s)").

72. One or more Forcepoint subsidiaries and/or affiliates use the Forcepoint '431 Products in regular business operations.

73. One or more of the Forcepoint '431 Products include technology for managing data traffic comprising a plurality of micro-flows through a network.

74. One or more of the Forcepoint '431 Products determine the capacity of a buffer containing a micro-flow based on a characteristic.

75. One or more of the Forcepoint '431 Products assign an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

76. One or more of the Forcepoint '431 Products delegate a portion of available bandwidth in the network to the micro-flow.

77. The Forcepoint '431 Products enable the setting of thresholds for a buffer that include the ability to set a threshold as a percentage of the buffer.

78. One or more of the Forcepoint '431 Products use the buffer for damping jitter associated with the micro-flow.

79. The Forcepoint '431 Products use buffers to limit jitter which is delay variance.

80. Forcepoint has directly infringed and continues to directly infringe the '431 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Forcepoint '431 Products.

81. The Forcepoint '431 Products are available to businesses and individuals throughout the United States.

82. The Forcepoint '431 Products are provided to businesses and individuals located in the Western District of Texas.

83. By making, using, testing, offering for sale, and/or selling products and services for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Forcepoint '431 Products, Forcepoint has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '431 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

84. Forcepoint also indirectly infringes the '431 patent by actively inducing infringement under 35 USC § 271(b).

85. Forcepoint has had knowledge of the '431 patent since at least service of this Complaint or shortly thereafter, and Forcepoint knew of the '431 patent and knew of its infringement, including by way of this lawsuit.

86. Forcepoint intended to induce patent infringement by third-party customers and users of the Forcepoint '431 Products and had knowledge that the inducing acts would cause

infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Forcepoint specifically intended and was aware that the normal and customary use of the accused products would infringe the '431 patent. Forcepoint performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '431 patent and with the knowledge that the induced acts would constitute infringement. For example, Forcepoint provides the Forcepoint '431 Products that have the capability of operating in a manner that infringe one or more of the claims of the '431 patent, including at least claim 1, and Forcepoint further provides documentation and training materials that cause customers and end users of the Forcepoint '431 Products to utilize the products in a manner that directly infringe one or more claims of the '431 patent.[19] By providing instruction and training to customers and end-users on how to use the Forcepoint '431 Products in a manner that directly infringes one or more claims of the '431 patent, including at least claim 1, Forcepoint specifically intended to induce infringement of the '431 patent. Forcepoint engaged in such inducement to promote the sales of the Forcepoint '431 Products, e.g., through Forcepoint user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '431 patent. Accordingly, Forcepoint has induced and continues to induce users of

[19] *See, e.g.*, *Forcepoint Next Generation Firewall Product Guide Version 6.6 Revision A*, FORCEPOINT DOCUMENTATION (2019); *Forcepoint Intrusion Prevent System Datasheet,* FORCEPOINT DOCUMENTATION (2017); *Forcepoint Next Generation Firewall Product Guide Version 6.5 Revision A*, FORCEPOINT DOCUMENTATION (2018); *Forcepoint Firewall Enterprise Appliance Characterize and Contain Every New Threat and Vulnerability – Forcepoint Datasheet*, FORCEPOINT DOCUMENTATION (2016); *Forcepoint Next Generation Firewall Product Guide 6.2 Revision B*, FORCEPOINT DOCUMENTATION (2018); *Forcepoint Next Generation Firewall 6.8.3 Release Notes Revision A,* FORCEPOINT DOCUMENTATION (2020); *User Activity Monitoring | Forcepoint Insider Threat*, FORCEPOINT TECH TALK YOUTUBE CHANNEL (March 10, 2017), *available at*: https://www.youtube.com/watch?v=qSHexqYW-jE; *Forcepoint Stonesoft Next Generation Firewall Release Notes 6.6.1 Rev. A,* FORCEPOINT DOCUMENTATION (2019); and *Forcepoint Next Generation Firewall Online Help – Quality of Service and Bandwidth Management*, FORCEPOINT ONLINE HELP WEBSITE (last visited March 2021), *available at*: http://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.2.0/GUID-0AC5CAA5-018B-4CB2-BE7A-943378EDD97C.html.

the accused products to use the accused products in their ordinary and customary way to infringe the '431 patent, knowing that such use constitutes infringement of the '431 patent.

87. The '431 patent is well-known within the industry as demonstrated by multiple citations to the '431 patent in published patents and patent applications assigned to technology companies and academic institutions. Forcepoint is utilizing the technology claimed in the '431 patent without paying a reasonable royalty. Forcepoint is infringing the '431 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

88. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '431 patent.

89. As a result of Forcepoint's infringement of the '431 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Forcepoint's infringement, but in no event less than a reasonable royalty for the use made of the invention by Forcepoint together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,977,932

90. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

91. Forcepoint designs, makes, sells, offers to sell, imports, and/or uses the Forcepoint Next Generation Firewall (NGFW) Appliances running Forcepoint NGFW 6.0 and later software, including but not limited to the following: Forcepoint NGFW Appliances (including the following models: NGFW 5206 Appliance, NGFW 1401 Appliance, NGFW 3207 Appliance, NGFW 320X Appliance, NGFW 1402 Appliance, NGFW 1035 Appliance, NGFW 1065 Appliance, NGFW 321 Appliance, NGFW 325 Appliance, NGFW 110 Appliance, NGFW 115 Appliance, NGFW 331

Appliance, NGFW 335W Appliance, NGFW 51 Appliance, NGFW 51 LTE Appliance, NGFW 3301 Appliance, NGFW 3305 Appliance, NGFW 6205 Appliance, NGFW 2101 Appliance, NGFW 2105 Appliance, NGFW SMC 1000 Appliance, NGFW 1101 Appliance, NGFW 1105 Appliance, NGFW 330 Appliance, NGFW 335 Appliance, NGFW 3401 Appliance, NGFW 3405 Appliance, NGFW 3410 Appliance, NGFW 120W Appliance, and NGFW 60 Appliance); Forcepoint S Series Appliance (including the following models: Storage Array 30TB, Storage Array 110TB, and Storage Array 60TB); Forcepoint V10000 Series Appliance (including the following models: V10000 G4 R2, V10000 G4, V20000 G1, V5000 G3, V5000 G4, and V5000 G4 R2); Forcepoint X Series Appliance (including the following models: X10G Blade G2 R2 and X10G Blade G2); and Forcepoint Z Series Appliance (including the following models: Z2500 G1.2, Z5000 G1.2, Z10000 G1.2, Z20000 G1.2, Z50000 G1.2, Z2500 G1.1, Z5000 G1.1, Z10000 G1.1, Z20000 G1.1, Z50000 G1.1, Z2500 G1.0, Z5000 G1.0, Z10000 G1.0, Z20000 G1.0, and Z50000 G1.0) (collectively, the "Forcepoint '932 Products(s)").

92. One or more Forcepoint subsidiaries and/or affiliates use the Forcepoint '932 Products in regular business operations.

93. Forcepoint has directly infringed and continues to directly infringe the '932 patent by, among other things, making, using, offering for sale, and/or selling technology that utilize flow state information to perform a method of network tunneling.

94. One or more of the Forcepoint '932 Products utilize flow state information to perform a network tunneling method.

95. One or more of the Forcepoint '932 Products create a flow block having flow state information for a received first data packet of a micro-flow.

96. One or more of the Forcepoint '932 Products store a tunnel identifier for the micro-flow in the flow block, the tunnel identifier identifying a selected network tunnel to be used to transmit the data packet.

97. One or more of the Forcepoint '932 Products index an aggregate flow block using the tunnel identifier.

98. One or more of the Forcepoint '932 Products utilize an aggregate flow block with tunnel specific information for the selected network tunnel and that stores statistics for the selected network tunnel.

99. One or more of the Forcepoint '932 Products transmit data packets using the selected network tunnel based on the tunnel specific information.

100. The Forcepoint '932 Products are available to businesses and individuals throughout the United States.

101. The Forcepoint '932 Products are provided to businesses and individuals located in the Western District of Texas.

102. By making, using, testing, offering for sale, and/or selling products utilizing flow state information to perform a method of network tunneling, including but not limited to the Forcepoint '932 Products, Forcepoint has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '932 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

103. Forcepoint also indirectly infringes the '932 patent by actively inducing infringement under 35 USC § 271(b).

104. Forcepoint has had knowledge of the '932 patent since at least service of this Complaint or shortly thereafter, and Forcepoint knew of the '932 patent and knew of its infringement, including by way of this lawsuit.

105. Forcepoint intended to induce patent infringement by third-party customers and users of the Forcepoint '932 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Forcepoint specifically intended and was aware that the normal and customary use of the accused products would infringe the '932 patent. Forcepoint performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '932 patent and with the knowledge that the induced acts would constitute infringement. For example, Forcepoint provides the Forcepoint '932 Products that have the capability of operating in a manner that infringe one or more of the claims of the '932 patent, including at least claim 1, and Forcepoint further provides documentation and training materials that cause customers and end users of the Forcepoint '932 Products to utilize the products in a manner that directly infringe one or more claims of the '932 patent.[20] By providing instruction and training to customers and

[20] *See, e.g.*, *Forcepoint Next Generation Firewall Product Guide Version 6.7 Revision A,* FORCEPOINT DOCUMENTATION (2019); *Forcepoint Next Generation Firewall (NGFW): Connect and product Your People and Their Data Throughout Your Enterprise Network,* FORCEPOINT DOCUMENTATION (2017); *NGFW SMC API for Forcepoint Next Generation Firewall Reference Guide Version 6.3 Revision A,* FORCEPOINT DOCUMENTATION (2017); *Forcepoint Next Generation Firewall Product Guide Version 6.6 Revision A*, FORCEPOINT DOCUMENTATION (2019); *Forcepoint Intrusion Prevention System Datasheet,* FORCEPOINT DOCUMENTATION (2017); *Forcepoint Next Generation Firewall Product Guide Version 6.5 Revision A*, FORCEPOINT DOCUMENTATION (2018); *Forcepoint Firewall Enterprise Appliance: Characterize and Contain Every New Threat and Vulnerability – Forcepoint Datasheet*, FORCEPOINT DOCUMENTATION (2016); *Forcepoint Next Generation Firewall Product Guide 6.2 Revision B*, FORCEPOINT DOCUMENTATION (2018); *Forcepoint Next Generation Firewall 6.8.3 Release Notes Revision A,* FORCEPOINT DOCUMENTATION (2020); *User Activity Monitoring | Forcepoint Insider Threat*, FORCEPOINT TECH TALK YOUTUBE CHANNEL (March 10, 2017), *available at*: https://www.youtube.com/watch?v=qSHexqYW-jE; *Forcepoint Stonesoft Next Generation Firewall Release Notes 6.6.1 Rev. A,* FORCEPOINT DOCUMENTATION (2019); and *Forcepoint Next Generation Firewall Online Help – Quality of Service and Bandwidth Management*, FORCEPOINT ONLINE HELP WEBSITE (last visited March 2021),

end-users on how to use the Forcepoint '932 Products in a manner that directly infringes one or more claims of the '932 patent, including at least claim 1, Forcepoint specifically intended to induce infringement of the '932 patent. Forcepoint engaged in such inducement to promote the sales of the Forcepoint '932 Products, e.g., through Forcepoint user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '932 patent. Accordingly, Forcepoint has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '932 patent, knowing that such use constitutes infringement of the '932 patent.

106. The '932 patent is well-known within the industry as demonstrated by multiple citations to the '932 patent in published patents and patent applications assigned to technology companies and academic institutions. Forcepoint is utilizing the technology claimed in the '932 patent without paying a reasonable royalty. Forcepoint is infringing the '932 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

107. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '932 patent.

108. As a result of Forcepoint's infringement of the '932 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Forcepoint's infringement, but in no event less than a reasonable royalty for the use made of the invention by Forcepoint together with interest and costs as fixed by the Court.

---

available at: http://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.2.0/GUID-0AC5CAA5-018B-4CB2-BE7A-943378EDD97C.html.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 8,243,593

109. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

110. Forcepoint designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for processing a flow of a series of information packets.

111. Forcepoint designs, makes, sells, offers to sell, imports, and/or uses Forcepoint devices that contain Sidewinder Version 8.0 and later security functionality, including but not limited to the following products: Sidewinder 1402C3 Appliance, Sidewinder S1104 Appliance, Sidewinder S2008 Appliance, Sidewinder S4016 Appliance, Sidewinder S3008 Appliance, Sidewinder S5032 Appliance, Sidewinder S6032 Appliance, Sidewinder S7032 Appliance, Sidewinder for BlueCoat X-50 and X-80 Chassis All Software Versions, Sidewinder 4150F Appliance, Sidewinder 2150F Appliance, Sidewinder 1100F Appliance, Sidewinder 2100F Appliance, Sidewinder 2150F VX Appliance, Sidewinder 410F Appliance, and the Sidewinder 510F Appliance (collectively, the "Forcepoint '593 Product(s)").

112. One or more Forcepoint subsidiaries and/or affiliates use the Forcepoint '593 Products in regular business operations.

113. One or more of the Forcepoint '593 Products include technology for processing a flow of a series of information packets. Specifically, the Forcepoint '593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

114. The Forcepoint '593 Products are available to businesses and individuals throughout the United States.

115. The Forcepoint '593 Products are provided to businesses and individuals located in the Western District of Texas.

116. Forcepoint has directly infringed and continues to directly infringe the '593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

117. The Forcepoint '593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

118. The Forcepoint '593 Products enable the generation of behavioral statistics based on each packet that is processed.

119. The Forcepoint '593 Products determine, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

120. The Forcepoint '593 Products determine whether the flow is exhibiting undesirable behavior regardless of the presence or absence of congestion.

121. The Forcepoint '593 Products enforce a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

122. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the Forcepoint '593 Products, Forcepoint has injured Plaintiffs and is liable for directly infringing one or more claims of the '593 patent, including at least claim 4, pursuant to 35 U.S.C. § 271(a).

123. Forcepoint also indirectly infringes the '593 patent by actively inducing infringement under 35 USC § 271(b).

124. Forcepoint has had knowledge of the '593 patent since at least service of this Complaint or shortly thereafter, and Forcepoint knew of the '593 patent and knew of its infringement, including by way of this lawsuit.

125. Forcepoint intended to induce patent infringement by third-party customers and users of the Forcepoint '593 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Forcepoint specifically intended and was aware that the normal and customary use of the accused products would infringe the '593 patent. Forcepoint performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '593 patent and with the knowledge that the induced acts would constitute infringement. For example, Forcepoint provides the Forcepoint '593 Products that have the capability of operating in a manner that infringe one or more of the claims of the '593 patent, including at least claim 4, and Forcepoint further provides documentation and training materials that cause customers and end users of the Forcepoint '593 Products to utilize the products in a manner that directly infringe one or more claims of the '593 patent.[21] By providing instruction and training to customers and end-users on how to use the Forcepoint '593 Products in a manner that directly infringes one or more claims of the '593 patent, including at least claim 4, Forcepoint specifically intended to induce infringement of the '593 patent. Forcepoint engaged in such inducement to promote the sales of the Forcepoint '593 Products, e.g., through Forcepoint user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '593 patent. Accordingly, Forcepoint has induced and continues to induce users of

[21] *See, e.g.*, *Forcepoint Sidewinder Product Guide 8.3.2P03 and later Revision A,* FORCEPOINT DOCUMENTATION (2016); *Forcepoint Sidewinder Administration Guide 7.0.1.3H14,* FORCEPOINT DOCUMENTATION (2016); *Forcepoint Sidewinder Product Guide 8.3.2P03 and later Revision C,* FORCEPOINT DOCUMENTATION (2017); *Forcepoint Sidewinder Product Guide 8.3.2P03 and later Revision B,* FORCEPOINT DOCUMENTATION (2016); *Forcepoint Advanced Classification Engine (ACE) Solution Brief,* FORCEPOINT DOCUMENTATION (2020); Kaan Kayan, *Forcepoint UEBA User & Entity Behavior Analytics Presentation*, FORCEPOINT DOCUMENTATION (2017); *Forcepoint UEBA User Manual v3.0.x,* FORCEPOINT DOCUMENTATION (July 10, 2018); and *Forcepoint Behavioral Analytics: Platform Architecture Overview: From Data to Behavior Insights – Functional Architectures*, FORCEPOINT DATASHEET (2020).

the accused products to use the accused products in their ordinary and customary way to infringe the '593 patent, knowing that such use constitutes infringement of the '593 patent.

126. The '593 patent is well-known within the industry as demonstrated by multiple citations to the '593 patent in published patents and patent applications assigned to technology companies and academic institutions. Forcepoint is utilizing the technology claimed in the '593 patent without paying a reasonable royalty. Forcepoint is infringing the '593 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

127. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '593 patent.

128. As a result of Forcepoint's infringement of the '593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Forcepoint's infringement, but in no event less than a reasonable royalty for the use made of the invention by Forcepoint together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 9,774,501

129. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

130. Forcepoint designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for detecting outlier users of a network resource.

131. Forcepoint designs, makes, sells, offers to sell, imports, and/or uses the Forcepoint Cloud Access Security Broker (CASB) (including the Forcepoint Cloud Governance, Forcepoint Cloud Audit & Protection, and Forcepoint Cloud Security Suite products) (collectively, the "Forcepoint '501 Products").

132. The Forcepoint '501 Products perform the method of monitoring stream data associated with a user or device's usage of a network resource for a predetermined time.

133. The Forcepoint '501 Products perform the step of deriving a flow-count history. The flow-count history is generated based on stream data where a flow is a connection between a source IP address and a transport layer port to a destination IP address and transport layer port in which all of the packets use the same protocol.

134. The Forcepoint '501 Products perform the step of applying an outlier detection algorithm to the generated flow-count history associated with a user or a device and comparing the flow-count history to flow-count histories associated with other users or devices on the network.

135. The Forcepoint '501 Products assign a flow-count band to the user based on the outlier detection algorithm and flow-count history.

136. One or more of the Forcepoint '501 Products include technology for tracking flow data of a user subscriber for a predetermined time interval.

137. One or more of the Forcepoint '501 Products include functionality for aggregating flow data of a user for a number of time periods. The flow data that is aggregated by the Forcepoint '501 Products includes network communications between a particular source IP address and transport layer port to a particular destination IP address and transport layer port in which all of the packets are using the same protocol.

138. One or more of the Forcepoint '501 Products generate a flow-count pattern where the flow-count pattern is the count of the number of flows the user initiates as either the source IP address or destination IP address during a predetermined time period.

139. One or more of the Forcepoint '501 Products apply an outlier detection logic (algorithm) to the flow-count pattern as compared to a plurality of other flow-count patterns associated with a plurality of other users.

140. One or more of the Forcepoint '501 Products apply a mitigating action to the user concerning the user's access to the network resource based on the flow-count band assigned.

141. The Forcepoint '501 Products are available to businesses and individuals throughout the United States.

142. The Forcepoint '501 Products are provided to businesses and individuals located in the Western District of Texas.

143. Forcepoint has directly infringed and continues to directly infringe the '501 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Forcepoint '501 Products.

144. By making, using, testing, offering for sale, and/or selling products and services for detecting outlier users of a network resource, including but not limited to the Forcepoint '501 Products, Forcepoint has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '501 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

145. Forcepoint indirectly infringes the '501 patent, including at least claim 1, by actively inducing infringement under 35 U.S.C. § 271(b).

146. Forcepoint has had knowledge of the '501 patent since at least service of this Complaint or shortly thereafter, and Forcepoint knew of the '501 patent and knew of its infringement, including by way of this lawsuit.

147. Forcepoint intended to induce patent infringement by third-party customers and users of the Forcepoint '501 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Forcepoint specifically intended and was aware that the normal and customary use of the accused products would infringe the '501 patent. Forcepoint performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '501 patent and with the knowledge that the induced acts would constitute infringement. For example, Forcepoint provides the Forcepoint '501 Products that have the capability of operating in a manner that infringe one or more of the claims of the '501 patent, including at least claim 1, and Forcepoint further provides documentation and training materials that cause customers and end users of the Forcepoint '501 Products to utilize the products in a manner that directly infringe one or more claims of the '501 patent.[22] By providing instruction and training to customers and end-users on how to use the Forcepoint '501 Products in a manner that directly infringes one or

[22] *See, e.g.*, *Forcepoint CASB – Product Feature Comparison,* FORCEPOINT SPECIFICATIONS SHEET (2017); *Forcepoint CASB Administration Guide Version 2020 R4,* FORCEPOINT DOCUMENTATION (December 13, 2020); *Forcepoint NGFW Integration with Forcepoint CASB,* FORCEPOINT TECHNICAL DOCUMENT (2018); Jack Poller and Alex Arcilla, *Forcepoint Cloud Access Security Broker (CASB): Securing the Use of Cloud Applications,* ESG LAB VALIDATION DOCUMENT (2018) ("This ESG Lab Reports was commissioned by Forcepoint"); *Forcepoint Cloud Threat Assessment Report Introduction and FAQ,* FORCEPOINT CASB DOCUMENTATION (2018); Kfir Mesika, *Protecting Your Cloud Journey @DLP @CASB @SD-WAN,* FORCEPOINT DOCUMENTATION (2019); *Forcepoint CASB – Forcepoint Web Security Integration Guide Version 2018 R4*, FORCEPOINT DOCUMENTATION (2018); Nitzan Cohen, *Forcepoint Israel Tech Week Presentation,* FORCEPOINT DOCUMENTATION (September 2020); Rob Mathieson, *Forcepoint Dynamic Data Protection Automated Policy Enforcement Through Practical Application of Risk Modeling,* FORCEPOINT DOCUMENTATION (2019); Brijesh Miglani, *A Human-Centric Approach to Risk Adaptive Cybersecurity,* FORCEPOINT PRESENTATION (2020); Victor Martinez, *Forcepoint's Approach to Zero Trust (ZTX) - A Data-Centric Security Architecture, Protected By Behavior-Based Controls*, FORCEPOINT PRESENTATION (2019); *Forcepoint Cloud Control: Get The Visibility and Control You Need To Secure Data In The Cloud*, FORCEPOINT GARTNER RESEARCH PUBLICATION (2018); and David Coffey, *Forcepoint Cloud Application Security Broker and Web Security*, TECH FIELD DAY YOUTUBE CHANNEL (February 23, 2018), *available at*: https://www.youtube.com/watch?v=8_3M_DNruWY (presentation is from Forcepoint's VP of Research and Development).

more claims of the '501 patent, including at least claim 1, Forcepoint specifically intended to induce infringement of the '501 patent. Forcepoint engaged in such inducement to promote the sales of the Forcepoint '501 Products, e.g., through Forcepoint user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '501 patent. Accordingly, Forcepoint has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '501 patent, knowing that such use constitutes infringement of the '501 patent.

148. The '501 patent is well-known within the industry as demonstrated by multiple citations to the '501 patent in published patents and patent applications assigned to technology companies and academic institutions. Forcepoint is utilizing the technology claimed in the '501 patent without paying a reasonable royalty. Forcepoint is infringing the '501 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

149. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '501 patent.

150. As a result of Forcepoint's infringement of the '501 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Forcepoint's infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

A. A judgment in favor of Plaintiffs that Forcepoint has infringed, either literally and/or under the doctrine of equivalents, the '431, '932, '593, and '501 patents;

B. An award of damages resulting from Forcepoint's acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that Forcepoint's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys' fees against Forcepoint.

E. Any and all other relief to which Plaintiffs may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: March 10, 2021

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com

Attorneys for Sable Networks, Inc. and Sable IP, LLC